<div align="center">REMARKS</div>

This Response is submitted in reply to the Office Action dated June 20, 2007, issued in connection with the above-identified application. Claims 1-23 are pending in the application. Claims 1, 5, 13, 14 and 20-23 have been amended. No new matter has been introduced; thus, reconsideration is respectfully requested. Applicants thank the Examiner for conducting the Examiner's Interview on October 18, 2007.

35 USC §112 Rejections

The Office Action rejects Claims under 35 USC 112 first paragraph as failing to comply with the written description requirement, specifically "comparing the decrypted result with the first data item" and "wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item." Applicants respectfully submit that Claims 1, 5, 13, 14 and 20-23 have been amended to traverse such rejections.

Claim 1 now reads, in part, "wherein, only when the user has been authenticated in response to the additional authentication request, the authentication apparatus performs processing, using the private key corresponding to the user, to decrypt transaction information sent from the information processing apparatus to the data holding medium~~authenticate the~~ ~~user~~," and "wherein said information processing apparatus is configured to decrypt the encrypted first data item using a public key associated with the user and to ensure that the decryption is successfully performed ~~and to compare the decrypted result with the first data item~~." Claims 5, 13, 14 and 20-23 contain similar language.

The Office Action states that the disclosure fails to recite "comparing the decrypted result with the first data item" and "wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item." The Office Action, states that there is no disclosure of comparing the decrypted digital signature with a previous digital signature. Applicants submit that the amended Claims are fully supported by the specification. For example, see the specification in paragraph .

Further, in paragraph 65, the specification states, in part, "When the WWW server 3 receives the digital signature sheet, the WWW server decrypts the digital signature by using the public key written into the user certificate received in advance. When the **decryption is**

successfully performed, it is determined that the legitimate user terminal 4 has requested the electronic priced information." (emphasis added).

After successfully authenticating the IC card, the authentication apparatus decrypts the encrypted electronic priced information using the private key as claimed in amended Claim 1, "wherein, only when the user has been authenticated in response to the additional authentication request, the authentication apparatus performs processing, using the private key corresponding to the user, to decrypt transaction information sent from the information processing apparatus to the data holding medium~~authenticate the user~~, wherein transaction information encrypted by the public-key encryption method, which is sent from the information processing apparatus and forwarded to the authentication apparatus, is decrypted by the authentication apparatus using the private key corresponding to the user so as to obtain decrypted transaction information." The data was encrypted using the public key and then after the IC card is authenticated, the information is decrypted using the private key and transmitted to the IC card as shown in paragraph 74.

For at least the foregoing reasons, Applicants respectfully submit that the rejections have been traversed and that Claims 1-21 are in condition for allowance with respect to the 35 USC §112 rejections.

35 USC 103 Rejections

The Office Action rejects Claims 1-23 under 35 USC 103(a) as being unpatentable over Audebert (US Patent No. 6,694,436) in view of Carden (GB 2261538). Applicants respectfully disagree and traverse such rejections.

The Office Action states that the reference Audebert discloses, "said authentication apparatus for holding the common key used in the common-key encryption method and a private key corresponding to the user used in a public-key encryption method for authentication between the data holding medium and a server to perform a service to the user." Applicants respectfully disagree. The data card of Audebert stores the private key, not the authentication apparatus. For example, see Audebert column 22 lines 1-2, "the terminal module 1 sends a private key read request to the card." The claimed data recording medium stores the common key but does **not** store the private key. Audebert teaches away from storing the private key externally from the

data card. For example, see Audebert in column 21, lines 28-34 stating, in part, "The principle of operation is as follows: the transaction is signed by the terminal module 1 **using a private key held by the card 31**." Additionally, column 22, lines 7-10 stating, "the terminal module 1 decrypts the private key, signs the transaction by means of the private key, **destroys the private key**, disconnects from the card 31 and sends the signed transaction to the PC which sends it to the server S." Audebert is directed towards a system where the private key is stored on the card for security purposes. However, the claims are directed towards an authentication apparatus storing the private key, and the data medium holding the common key.

Additionally, Audebert does not disclose or suggest the additional public key encryption of the electronic pricing information by the information processing apparatus, common-key authentication by the security server and decryption by the security server. The Office Action suggests that it would be obvious to encrypt the data from the information processing apparatus of Audebert. However, encrypting and decrypting the data twice, first between the security server and the information processing apparatus using the public key method, and then between the security server and the data holding medium using the common key encryption method, would not be obvious.

The reference Carden cannot be relied upon to cure the deficiencies of Audebert. For at least the foregoing reasons, Applicants respectfully submit that Claims 1, 5, 13, 14 and 20-23, and Claims 2-4, 6-12 and 15-19 that depend therefrom, are patentably distinguishable and in condition for allowance.

The Commissioner is hereby authorized to charge deposit account 02-1818 for any fees which are due and owing.

Respectfully submitted,

BELL, BOYD & LLOYD LLP

BY _____
Thomas C. Basso
Reg. No. 46,541
Customer No. 29175

Dated: October 23, 2007 _____

14